PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059357
(43)Date of publication of application : 25.02.2000

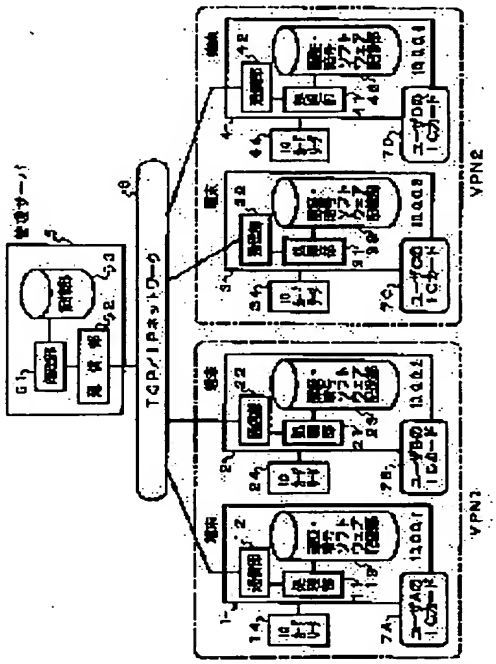
(51)Int.Cl. H04L 9/32
G09C 1/00
H04L 9/08
H04L 12/28

(21)Application number : 10-224079
(22)Date of filing : 07.08.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : OKA KATSUYA
CHITOKU SHINYA
SAIJO TOMOYUKI
ONO HIROYASU

(54) CLOSED AREA GROUP COMMUNICATION SYSTEM, MANAGEMENT SERVER SYSTEM, COMMUNICATION TERMINAL AND THEIR PROGRAM STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To build up a virtual private network VPN independently of a physical condition of a network such as a terminal utilizing IP address and a work place for the user in the case of building up the virtual private network VPN on the network using the TCP/IP.
SOLUTION: User Ids and passwords of all users using a network are registered by a management server 5 and an IC card 7 (A-D) is distributed to all the users. Furthermore, an authentication/encryption software and an IC card reader are provided to all terminals 1-4 on the network. The management server 5 configures a VPN in the unit of the user Ids and each user when using the network uses the IC card of the terminal and the user ID/password to receive the authentication by the management server 5. In this case, the management server 5 registers the IP address of the user terminal made to correspond to the VPN to which the user belongs so as to allow terminals used by users belonging to the same VPN to configure the VPN.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－59357
（P2000－59357A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
H04L	9/32		H04L	9/00	675D	5J104
G09C	1/00	620	G09C	1/00	620Z	5K033
H04L	9/08		H04L	9/00	601D	
	12/28				673A	
				11/00	310D	

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

(21)出願番号　特願平10－224079

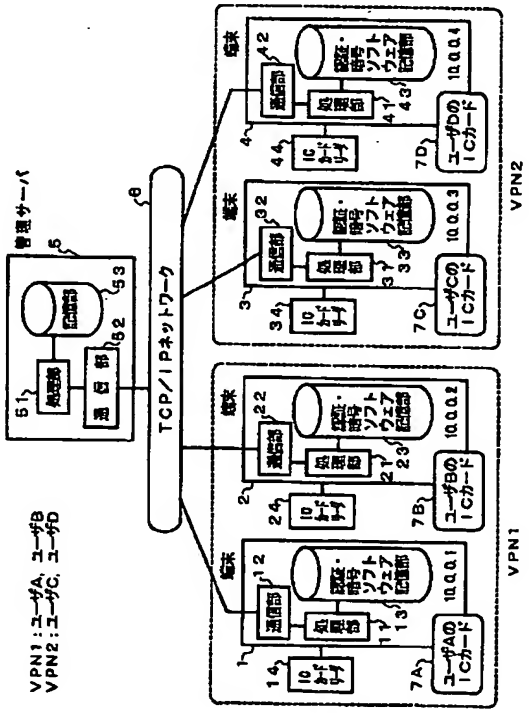
(22)出願日　平成10年８月７日(1998.8.7)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　岡　克也
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　千徳　真也
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100087848
弁理士　小笠原　吉義　（外１名）

最終頁に続く

(54)【発明の名称】　閉域グループ通信システム，管理サーバ装置および通信端末，ならびにそれらのプログラム記憶媒体

(57)【要約】
【課題】ＴＣＰ／ＩＰを利用するネットワーク上で，仮想的な閉域グループ（ＶＰＮ）を構築する際に，端末の利用ＩＰアドレスや利用者の作業場所など，ネットワークの物理的条件に依存しないＶＰＮを構築可能にする。
【解決手段】管理サーバ５に，ネットワークを利用する全ユーザのユーザＩＤとパスワードを登録し，全ユーザにＩＣカード７を配布する。また，ネットワーク上の全端末１～４に，認証・暗号ソフトウェアとＩＣカードリーダを装備する。管理サーバ５において，ユーザＩＤを単位としてＶＰＮを構成し，ユーザはネットワーク利用時に端末からＩＣカードとユーザＩＤ・パスワードを利用して管理サーバ５にて認証を受ける。このとき，管理サーバ５がユーザ利用端末のＩＰアドレスをユーザの所属するＶＰＮに対応づけて登録することにより，同一ＶＰＮに所属するユーザが利用している端末がＶＰＮを構成する。



1

【特許請求の範囲】

【請求項１】　各ユーザが持つカード型記憶媒体と，該カード型記憶媒体の入出力インタフェースを有する通信端末と，通信ネットワークを介してそれらの通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を配布する管理サーバ装置から構成される閉域グループ通信システムであって，前記カード型記憶媒体は，前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵の情報を保持し，前記管理サーバ装置は，あらかじめ前記通信端末を利用する各ユーザに対して割り当てられたユーザＩＤとパスワードおよび複数の閉域グループ番号と閉域グループに属するユーザＩＤを管理記憶する手段と，前記通信端末から送信されてきたユーザＩＤとパスワードを，該管理サーバ装置の秘密鍵を用いて復号化し，ユーザＩＤとパスワードが認証できた場合には，該ユーザＩＤが属する閉域グループの通信用暗号鍵を該ユーザＩＤを持つユーザの公開鍵によって暗号化し，前記通信端末へ送信する手段とを備え，前記通信端末は，前記入出力インタフェースに差し込まれた前記カード型記憶媒体から，前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵を読み出す手段と，該管理サーバ装置の公開鍵を用いてユーザＩＤとパスワードを暗号化し，通信ネットワークを介して前記管理サーバ装置に送信する手段と，前記管理サーバ装置から送信されてきた閉域グループ内通信端末との通信用暗号鍵を受信して前記ユーザ個々の秘密鍵により復号化する手段と，該復号化した通信用暗号鍵を用いて通信端末相互における通信情報を暗号化し，閉域グループ内通信端末相互の通信を行う手段とを備えることを特徴とする閉域グループ通信システム。

【請求項２】　通信ネットワークを介して通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を配布する管理サーバ装置であって，あらかじめ閉域グループ内での通信を行う各ユーザに対して割り当てられたユーザＩＤとパスワードおよび複数の閉域グループ番号と閉域グループに属するユーザＩＤを管理記憶する手段と，前記ユーザが利用する通信端末から送られてきたユーザＩＤとパスワードであって，該通信端末が各ユーザにあらかじめ配布されたカード型記憶媒体から読み出した該管理サーバ装置の公開鍵を用いて暗号化したユーザＩＤとパスワードを，該管理サーバ装置の秘密鍵を用いて復号化し，ユーザＩＤとパスワードが認証できた場合には，該ユーザＩＤが属する閉域グループの通信用暗号鍵を該ユーザＩＤを持つユーザの公開鍵によって暗号化し，前記通信端末へ送信する手段とを備えることを特徴とする管理サーバ装置。

【請求項３】　管理サーバ装置から配布された通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を用いて，通信ネットワークを介して通信を行う通信端末であって，カード型記憶媒体の入出力インタフェースと，あらかじめ前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵の情報が格納されたカード型記憶媒体から，前記入出力インタフェースを介して前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵を読み出す手段と，該管理サーバ装置の公開鍵を用いてユーザＩＤとパスワードを暗号化し，通信ネットワークを介して前記管理サーバ装置に送信する手段と，前記管理サーバ装置から送信されてきた閉域グループ内通信端末との通信用暗号鍵を受信して前記ユーザ個々の秘密鍵により復号化する手段と，該復号化した通信用暗号鍵を用いて通信端末相互における通信情報を暗号化し，閉域グループ内通信端末相互の通信を行う手段とを備えることを特徴とする通信端末。

2

【請求項４】　通信ネットワークを介して通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を配布する管理サーバ装置が用いるプログラムを格納したプログラム記憶媒体であって，あらかじめ閉域グループ内での通信を行う各ユーザに対して割り当てられたユーザＩＤとパスワードおよび複数の閉域グループ番号と閉域グループに属するユーザＩＤを管理記憶する処理と，前記通信端末から送られてきた暗号化されたユーザＩＤとパスワードを，該管理サーバ装置の秘密鍵を用いて復号化する処理と，復号化されたユーザＩＤとパスワードを，あらかじめ登録されたユーザＩＤとパスワードとの照合により認証する処理と，ユーザＩＤとパスワードが認証できた場合に，該ユーザＩＤが属する閉域グループの通信用暗号鍵を該ユーザＩＤを持つユーザの公開鍵によって暗号化し，前記通信端末へ送信する処理とを，計算機に実行させるプログラムを格納したことを特徴とする管理サーバ装置のプログラム記憶媒体。

【請求項５】　管理サーバ装置から配布された通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を用いて，通信ネットワークを介して通信を行う通信端末が用いるプログラムを格納したプログラム記憶媒体であって，あらかじめ前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵の情報が格納されたカード型記憶媒体から，入出力インタフェースを介して前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵を読み出す処理と，該管理サーバ装置の公開鍵を用いてユーザＩＤとパスワードを暗号化し，通信ネットワークを介して前記管理サーバ装置に送信する処理と，前記管理サーバ装置から送信されてきた閉域グループ内通信端末との通信用暗号鍵を受信して前記ユーザ個々の秘密鍵により復号化する処理と，該復号化した通信用暗号鍵を用いて通信端末相互における通信情報を暗号化し，閉域グループ内通信端末相互の通信を行う処理とを，計算機に実行させるプログラムを格納したことを特徴とする通信端末のプログラム記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，ＴＣＰ／ＩＰプロ

3

トコルを利用して端末が相互に通信可能なネットワーク上に複数の仮想的な閉域グループ（以下，ＶＰＮという）を構築し，同一ＶＰＮに所属するユーザ間の通信のみ可能な環境を提供するＶＰＮ構築技術に係わり，特にＶＰＮがユーザの作業場所に依存しないようにした閉域グループ通信システム，管理サーバ装置および通信端末，ならびにそれらのプログラム記憶媒体に関するものである。

【０００２】

【従来の技術】ＴＣＰ／ＩＰネットワーク上でＶＰＮを構成する場合，従来は端末が利用しているＩＰアドレスを単位としてＶＰＮを構成していた。

【０００３】図１０は従来の第１のシステム構成例，図１１は従来の第２のシステム構成例を示す。図１０および図１１では，端末１０と端末２０とが同一のＶＰＮ１に属しており，端末３０と端末４０とが同一のＶＰＮ２に属している。管理サーバ５０は，これらのＶＰＮ情報を管理する。すなわち，それぞれの端末に固定的に割り当てられたＩＰアドレスと，ＶＰＮ１，ＶＰＮ２との対応関係を管理する。管理サーバ５０と各端末とは，ＴＣＰ／ＩＰネットワーク６０を介して接続される。

【０００４】図１０では，ユーザＡとユーザＢとは，同一のＶＰＮ１にあるＩＰアドレスの端末同士であると管理サーバ５０上で認識され通信することが可能であるが，図１１のようにユーザＢが作業場所を移動すると，管理サーバ５０上では，端末１０のＩＰアドレスと端末４０のＩＰアドレスとは異なったＶＰＮにあると認識されるので，ユーザＡはユーザＢと通信できない。

【０００５】

【発明が解決しようとする課題】従来技術では，ユーザが通常利用している端末から別の端末へ作業場所を移動した場合や，通常利用している端末を別のサブネットへ移動してＩＰアドレスが変わった場合には，ユーザが同一ＶＰＮでありながら異なったＶＰＮに所属する端末と通信不能になる。もし，このようなときに通信を行いたい場合には，ＶＰＮを構成する端末のＩＰアドレスの設定変更を，いちいちＶＰＮを管理する管理サーバ側で行うことが必要であった。

【０００６】本発明は上記問題点の解決を図り，ネットワーク上でＶＰＮを構築する際に，端末の利用ＩＰアドレスやユーザの作業場所など，ネットワークの物理的条件に依存しないＶＰＮを構築できるようにし，ユーザが作業場所を変えたり，また他の端末を利用した場合でも，ＩＰアドレスの設定変更を行うことなく，同一ＶＰＮに所属するユーザとの間でセキュアな通信を可能とすることを目的とする。

【０００７】

【課題を解決するための手段】本発明は，ユーザ全員にシステム内でユニークなユーザＩＤとパスワードを割り当て，管理サーバにおけるＶＰＮ構成単位を，従来の端末のＩＰアドレスからユーザＩＤへ変更し，ユーザＩＤと端末のＩＰアドレスの変換テーブルを管理することにより，物理的なネットワークに依存しないＶＰＮを構成可能にすることをもっとも主要な特徴とする。

【０００８】ユーザが通信ネットワークを利用する際に，ユーザＩＤとパスワードを用いて管理サーバによる認証を行う。認証時に，ユーザが利用する端末のＩＰアドレスを管理サーバに登録することにより，以降，従来のＩＰアドレスを単位としたＶＰＮの技術をそのまま用いることができる。

【０００９】また，認証にユーザＩＤとパスワードの他に，カード型記憶媒体（例えば，ＩＣカード）を併用することにより，安全な認証を可能とする。

【００１０】

【発明の実施の形態】［本発明の実施の形態の概要］本システムの前提条件として，任意の構成装置を用いた単一の閉域ネットワーク上で，端末は任意のサブネットに帰属しており，ＴＣＰ／ＩＰプロトコルを利用して相互に通信可能な環境となっているものとする。ネットワーク上の全ての端末からアクセス可能な管理サーバが一台存在し，ネットワークに接続する全端末には，認証・暗号ソフトウェアとＩＣカードリーダがインストールされているものとする。

【００１１】このような前提のもとで，全ネットワーク利用者（以下，ユーザという）に対して一意に英数字等からなるユーザＩＤとパスワードを割り当て，管理サーバに設定する。管理サーバ上で，相互に通信可能なユーザを，ユーザＩＤを用いてグループ化し，単一のネットワーク上に複数の仮想的な閉域グループ（ＶＰＮ）を作成する。ユーザがネットワークを利用する際に，ＩＣカードを端末のＩＣカードリーダに挿入し，ユーザＩＤおよびパスワードを利用して端末から認証を行うことにより，同一ＶＰＮに所属するユーザが利用する各端末がＶＰＮを構成するようにする。

【００１２】ユーザＩＤを用いたＶＰＮを構築することにより，作業端末の移動による影響を受けることなく，同一ＶＰＮに所属するユーザとの間でセキュアな通信が可能となる。

【００１３】［利用形態］図１は，本発明の実施の形態における第１のシステム構成例を示す。本システムでは，ユーザＡとユーザＢとが同一ＶＰＮに属しており，ユーザＣとユーザＤとが同一ＶＰＮに属している。管理サーバ５は，これらのＶＰＮ情報を記憶部５３に記憶し管理する。処理部５１は，管理サーバ５の処理を実行する部分，通信部５２はＴＣＰ／ＩＰネットワーク６を介して各端末１～４と通信を実行する部分である。

【００１４】各端末１～４は，端末における処理を実行する処理部１１～４１，ＴＣＰ／ＩＰネットワーク６を介して管理サーバ５や他の端末と通信を行う通信部１２～４２および処理部１１～４１が実行する認証・暗号ソ

5

フトウェアを記憶する認証・暗号ソフトウェア記憶部１３～４３を持つ。また，各端末１～４には，各ユーザＡ～Ｄが持つＩＣカード７Ａ～７Ｄを読み取るためのＩＣカードリーダ１４～４４が装備されている。

【００１５】図１ではユーザＡが端末１，ユーザＢが端末２，ユーザＣが端末３，ユーザＤが端末４で作業している。このとき，端末１と端末２は通信可能であり，端末３と端末４は通信可能である。しかし，それ以外の端末間での通信はできない。

【００１６】図２は，本発明の実施の形態における第２のシステム構成例を示す。図２では，図１のシステムの状態から，ユーザＡが端末１から端末３へ作業場所を移動し，ユーザＣが端末３から端末１へ作業場所を移動している。この場合，端末１と端末３は通信可能であり，端末２と端末４は通信可能である。しかし，端末１と端末２との間，端末３と端末４との間の通信はできない。

【００１７】このように，ＶＰＮを構成する端末がユーザの移動に合わせて変化するため，ユーザは作業場所に依存せずにＶＰＮ内での通信が可能である。

【００１８】［各部の働き］図１，図２に示すシステムにおける各部の働きは，以下のとおりである。

【００１９】(a) 管理サーバ５

・全ネットワーク利用者のユーザＩＤとパスワードと所属ＶＰＮの対応関係を管理する。

・全ネットワーク利用者のユーザＩＤとそれぞれのユーザの公開鍵の対応関係を管理する。

・端末からの要求に応じてユーザ認証を行う。

・認証に成功したら，ユーザが利用している端末のＩＰアドレスをユーザＩＤと対応づけて登録する。ユーザが利用している端末に対して，個々のＶＰＮ内通信に必要な通信用暗号鍵を配布する。

【００２０】(b) 認証・暗号ソフトウェア記憶部１３，２３，３３，４３

認証・暗号ソフトウェアは，ＴＣＰ／ＩＰネットワーク６に接続する全端末１～４に内蔵されている。ユーザＩＤとパスワードを暗号化し，管理サーバ５へ送信して認証を受ける。管理サーバ５から配布された通信用暗号鍵を用いて，通信パケットを暗号化し，ＶＰＮ内端末間相互の通信を行う。

【００２１】(c) ＩＣカード７Ａ～７Ｄ，ＩＣカードリーダ１４，２４，３４，４４

ネットワーク利用者毎に一枚のＩＣカード７Ａ～７Ｄを割り当てる。これらの各ＩＣカードには暗号鍵が格納されており，ユーザは認証時にＩＣカードを利用することによって，ユーザＩＤおよびパスワードの送信や，通信用暗号鍵の受信を安全に行うことができる。

【００２２】［特徴・利点］

・本システムを利用することにより，ユーザを単位としたＶＰＮを構成することができ，ＶＰＮ内のユーザ間での通信セキュリティが確保される。

6

・ユーザが作業場所を移動しても，同一ＶＰＮに所属するユーザ同士の通信および通信セキュリティが確保される。

・ＩＣカードを利用することにより，安全にユーザ認証を行うことができる。

【００２３】［処理の流れ］図３は，図１に示すシステムの実際の動作例を説明する図である。図４は，端末の処理フローチャート，図５は，管理サーバの処理フローチャートである。

【００２４】実際の動作を説明するに先立ち，簡単に前提について説明する。あらかじめＶＰＮ利用ユーザは，管理サーバ５にアクセスし，ユーザＩＤ，パスワード，および利用するＶＰＮ番号を登録しておくものとする。図６は，ＶＰＮ利用ユーザがあらかじめ管理サーバ５に登録したユーザＩＤとパスワードの例を示す。

【００２５】ＩＣカード７Ａ～７Ｄには，それぞれ，管理サーバ５の公開鍵および各ユーザ毎の秘密鍵が格納されている。例えば，ユーザＡのＩＣカード７Ａには，管理サーバ５の公開鍵とユーザＡの秘密鍵が格納され，ユーザＢのＩＣカード７Ｂには，管理サーバ５の公開鍵とユーザＢの秘密鍵が格納されている。端末と管理サーバ５間は公開鍵暗号化方式により暗号化・復号化を行うこととする。管理サーバ５には，管理サーバ５の秘密鍵およびユーザ毎の公開鍵が格納されている。図７は，管理サーバ５が管理するユーザ毎の公開鍵の例を示す。

【００２６】ユーザＡとユーザＢがＶＰＮ１に所属し，ユーザＣとユーザＤがＶＰＮ２に所属するように設定されている。設定内容は図６に示すとおりである。各ユーザＡ～Ｄには，ユーザＡのユーザＩＤがＵＳＥＲ－Ａ，パスワードがpasswd１，同様にユーザＢがＵＳＥＲ－Ｂ，ユーザＣがＵＳＥＲ－Ｃ，ユーザＤがＵＳＥＲ－Ｄというように，それぞれユーザＩＤが割り当てられている。

【００２７】なお，ＩＣカード７Ａ～７Ｄの発行・管理，および管理サーバ５とユーザ毎の公開鍵・秘密鍵の発行・管理は，管理サーバ５で行う形態でもよく，また，第三者機関が発行するものを入手・使用する形態でもよい。

【００２８】以下，図３に示す(1) ～(26)に従って，図１に示すシステムの動作を説明する。

(1) ユーザＡは，同じＶＰＮ内の他のユーザと通信を行いたい場合，端末１のＩＣカードリーダ１４へＩＣカード７Ａを挿入する。

(2) ＩＣカードリーダ１４により，ＩＣカード７Ａから管理サーバ５の公開鍵とユーザＡの秘密鍵を，端末１のメモリ上へ読み出す（図４のステップＳ１）。

(3) 端末１は，ユーザＡからユーザＩＤとパスワードを入力する（図４のＳ２）。

(4) 入力されたユーザＩＤとパスワードを，管理サーバ５の公開鍵で暗号化する（図４のＳ３）。

7

(5) 端末１は，管理サーバ５へ暗号化されたユーザＩＤとパスワードおよび端末１のＩＰアドレスを読み出して送信する（図４のＳ４）。
(6) 管理サーバ５は，端末１からの認証パケット（暗号化されたユーザＩＤとパスワード）を受け取り（図５のＳ２１），管理サーバ５の秘密鍵でユーザＩＤとパスワードを復号化する（図５のＳ２２）。
(7) 次に，管理サーバ５は，ユーザＩＤとパスワードを図６に示す登録内容と比較して認証を行う（図５のＳ２３）。
(8) 管理サーバ５は，この認証に成功すると，ユーザＡの所属しているＶＰＮを調べ，ユーザＡから送られてきた認証パケット中のソースＩＰアドレス10.0.0.1を，図６に示すテーブルのＩＰアドレス欄にＶＰＮ１と対応づけて登録する（図５のＳ２４）。なお，端末１から管理サーバ５へ送信する認証パケット中にＩＰアドレスが通信ソフトウェアにより自動設定されない場合には，端末１のＩＰアドレスを読み出して管理サーバ５へ送信する形でもよい。
(9) 管理サーバ５は，端末１がＶＰＮ１内で通信するために必要な通信用暗号鍵をユーザＡの公開鍵で暗号化する（図５のＳ２５）。この際，あらかじめ登録しているユーザＩＤ毎の公開鍵管理テーブル（図７）のデータを使用する。
(10) 管理サーバ５は，暗号化されたＶＰＮ１の通信用暗号鍵を端末１へ送信する（図５のＳ２６）。
(11) 端末1 は，暗号化されたＶＰＮ１の通信用暗号鍵を管理サーバ５から受信し（図４のＳ５），ユーザＡの秘密鍵で復号化する（図４のＳ６）。
(12) 端末１は，管理サーバ５に対して通信用暗号鍵の受信応答を返す（図４のＳ７）。
(13)～(24) 端末２で，ユーザＢがＩＣカード７ＢをＩＣカードリーダ２４に挿入することにより，ユーザＢに対する認証処理が同様に行われ，端末２にＶＰＮ１の通信用暗号鍵が配布される。
(25)～(26) 以上の処理により，端末１と端末２は，同じ通信用暗号鍵を持つＶＰＮ１を構成するので，以後，端末１と端末２間の通信は，ＶＰＮ１の通信用暗号鍵を用いたデータ暗号化によって行う（図４のＳ９）。なお，ＶＰＮ内の通信を行うユーザ同士のＩＰアドレスは，管理サーバ５にアクセスして入手することにより，端末１と端末２間の通信を行うことが可能である。
【００２９】ユーザＣとユーザＤに関しても，同様の処理を行うことにより，ＶＰＮ２が構成される。ユーザＡ，ユーザＢ，ユーザＣ，ユーザＤがそれぞれ認証を受けた後の管理サーバ５が管理する構成情報は，図８のように変化する。
【００３０】図１に示すシステム構成の状態から図２に示すシステム構成の状態に変化する場合には，以下の動作となる。図９は，ユーザＡとユーザＣが端末１，端末

8

３での作業を中止する時の動作について説明した図である。以下，図９に示す(1) ～(12)に従って，その動作を説明する。
(1) ユーザＡは，端末１のＩＣカードリーダ１４からＩＣカード７Ａを抜き取る。端末１は，このＩＣカード７Ａの抜き取りを検出する（図４のＳ１１）。
(2) これにより，端末１に対して，メモリ上に格納されている管理サーバ５の公開鍵とユーザＡの秘密鍵の削除要求が発生する。
(3) 端末１は，メモリ上から管理サーバ５の公開鍵とユーザＡの秘密鍵を削除する（図４のＳ１２）。
(4) 端末１は，管理サーバ５に対してユーザＡのＩＰアドレスクリア要求を送信する（図４のＳ１３）。
(5) 管理サーバ５は，端末１からのユーザＡのＩＰアドレスクリア要求を受信し（図５のＳ３１），ユーザＡのＩＰアドレスをクリアする（図５のＳ３２）。
(6) 管理サーバ５は，端末１へＩＰアドレスクリア応答を返す（図５のＳ３３）。
(7) ～(12) ユーザＣについても同様の処理を行う。
【００３１】以上により，端末１と端末３は，ユーザＡとユーザＣが認証を受ける前の状態に戻り，ＶＰＮの構成メンバーではなくなる。続いて，ユーザＡは端末３で認証を受け，ユーザＣは端末１で認証を受ける。このとき，端末２と端末３がＶＰＮ１を構成し，端末１と端末４がＶＰＮ２を構成する。これによって，ユーザＡとユーザＢ，ユーザＣとユーザＤはそれぞれのＶＰＮ内で通信可能となる。
【００３２】なお，以上の説明では，カード型記憶媒体としてＩＣカードを用いた例を説明したが，記憶媒体であれば磁気カードや光磁気記録カードその他の記憶媒体であっても実施可能である。また，端末は固定的なものである必要はなく，カード型記憶媒体リーダ／ライタが内蔵された携帯型のものであってもよく，通信ネットワークは有線／無線いずれの形態でも本発明は実施可能である。
【００３３】以上の各処理を，管理サーバ５および端末１～４のそれぞれの計算機によって実現するためのプログラムは，計算機が読み取り可能な可搬媒体メモリ，半導体メモリ，ハードディスクなどの適当な記憶媒体に格納することができる。
【００３４】
【発明の効果】以上説明したように，本発明によれば，ユーザを単位とした，ＩＰアドレスに依存しないＶＰＮが構成できる。したがって，利用者は作業場所に依存せず，同一ＶＰＮに所属するユーザ間で通信セキュリティが確保された通信が可能である。
【図面の簡単な説明】
【図１】本発明の実施の形態における第１のシステム構成例を示す図である。
【図２】本発明の実施の形態における第２のシステム構

9

成例を示す図である。

【図３】図１に示すシステムの実際の動作例を説明する図である。

【図４】端末の処理フローチャートである。

【図５】管理サーバの処理フローチャートである。

【図６】ＶＰＮ利用ユーザが管理サーバに登録したユーザＩＤとパスワードの例を示す図である。

【図７】管理サーバが管理するユーザ毎の公開鍵の例を示す図である。

【図８】管理サーバが管理するＶＰＮ構成情報の例を示す図である。

【図９】ユーザが端末での作業を中止する時の動作説明図である。

【図１０】従来の第１のシステム構成例を示す図である。

10

【図１１】従来の第２のシステム構成例を示す図である。

【符号の説明】

１，２，３，４　端末

１１，２１，３１，４１　処理部

１２，２２，３２，４２　通信部

１３，２３，３３，４３　認証・暗号ソフトウェア記憶部

１４，２４，３４，４４　ＩＣカードリーダ

５　管理サーバ

５１　処理部

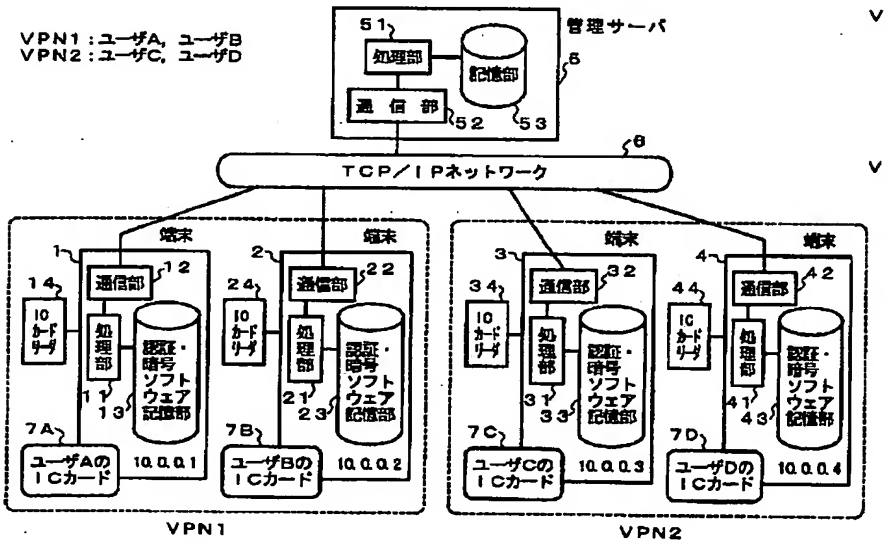
５２　通信部

５３　記憶部

６　ＴＣＰ／ＩＰネットワーク

７Ａ，７Ｂ，７Ｃ，７Ｄ　ＩＣカード

【図１】



【図６】

VPN1

ユーザＩＤ	パスワード	ＩＰアドレス
USER−A	passwd1	−
USER−B	passwd2	−

VPN2

ユーザＩＤ	パスワード	ＩＰアドレス
USER−C	passwd3	−
USER−D	passwd4	−

【図７】

ユーザＩＤ	公開鍵
USER−A	56978
USER−B	ab379
USER−C	xy115
⋮	⋮

【図８】

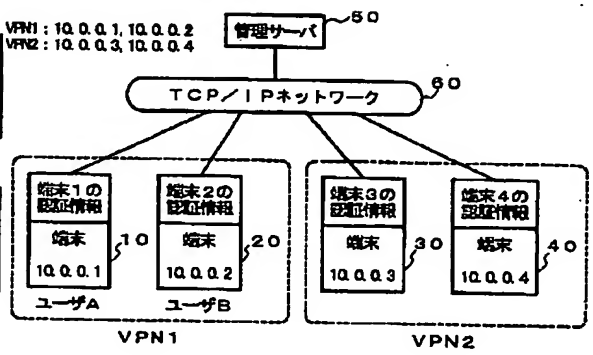
VPN1

ユーザＩＤ	パスワード	ＩＰアドレス
USER−A	passwd1	10.0.0.1
USER−B	passwd2	10.0.0.2

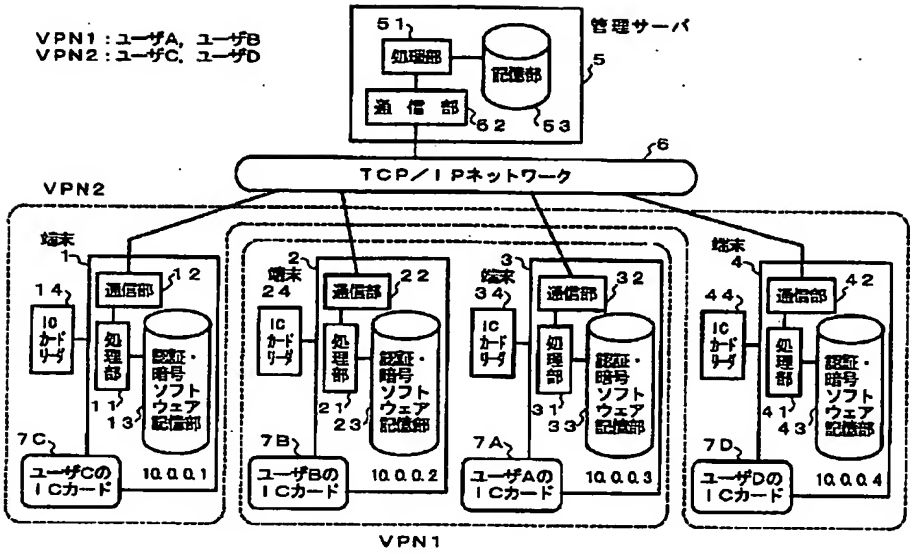
VPN2

ユーザＩＤ	パスワード	ＩＰアドレス
USER−C	passwd3	10.0.0.3
USER−D	passwd4	10.0.0.4

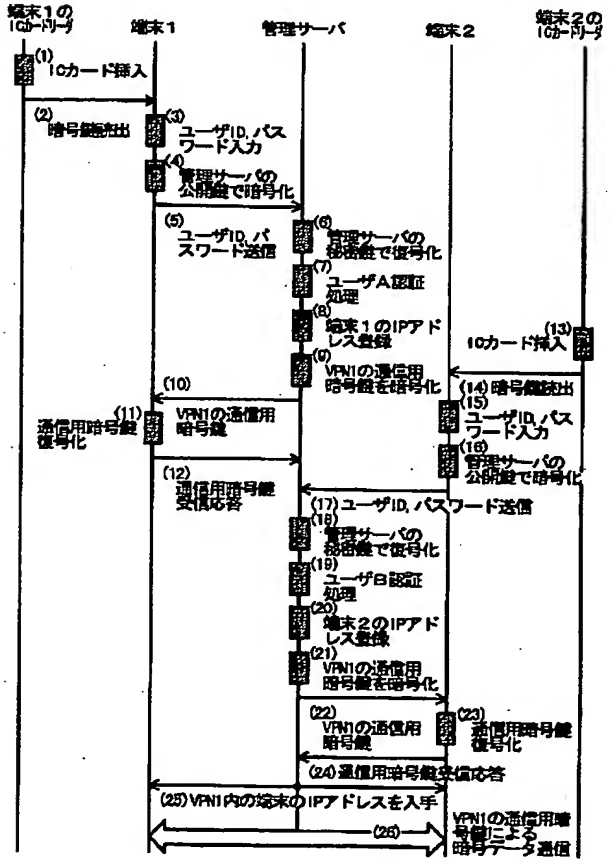
【図１０】



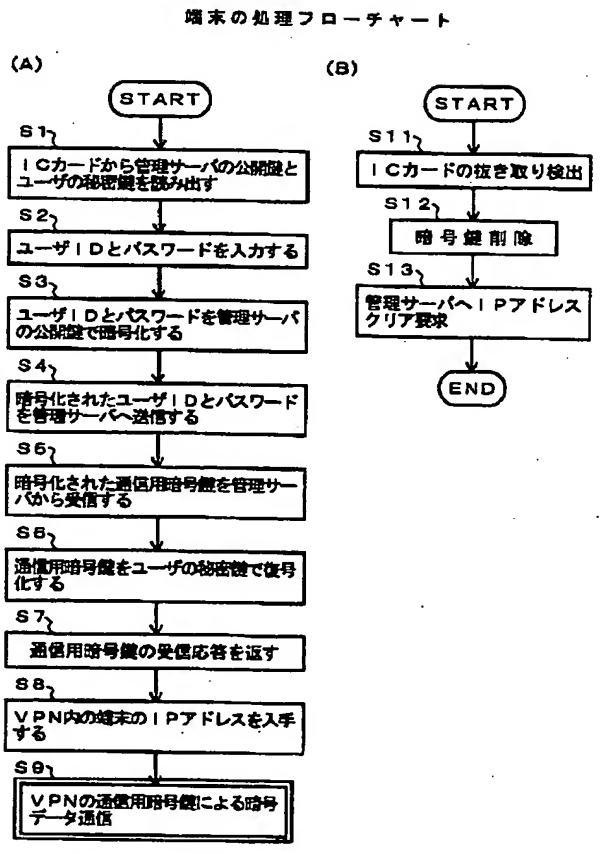
【図２】


VPN1：ユーザA，ユーザB
VPN2：ユーザC，ユーザD
管理サーバ
処理部
記憶部
通信部
TCP／IPネットワーク
VPN2
端末1
端末2
端末3
端末4
ICカードリーダ
通信部
処理部
認証・暗号ソフトウェア記憶部
ユーザCのICカード
ユーザBのICカード
ユーザAのICカード
ユーザDのICカード
10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
VPN1

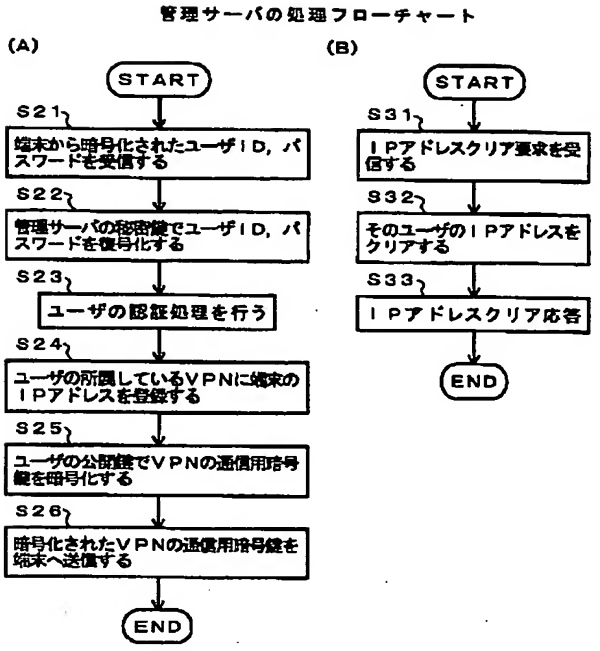
【図３】


端末1のICカードリーダ
端末1
管理サーバ
端末2
端末2のICカードリーダ
(1) ICカード挿入
(2) 暗号鍵生成
(3) ユーザID，パスワード入力
(4) 管理サーバの公開鍵で暗号化
(5) ユーザID，パスワード送信
(6) 管理サーバの秘密鍵で復号化
(7) ユーザA認証処理
(8) 端末1のIPアドレス登録
(9) VPN1の通信用暗号鍵を暗号化
(10)
(11) VPN1の通信用暗号鍵復号化
(12) 通信用暗号鍵受信応答
(13) ICカード挿入
(14) 暗号鍵生成
(15) ユーザID，パスワード入力
(16) 管理サーバの公開鍵で暗号化
(17) ユーザID，パスワード送信
(18) 管理サーバの秘密鍵で復号化
(19) ユーザB認証処理
(20) 端末2のIPアドレス登録
(21) VPN1の通信用暗号鍵を暗号化
(22) VPN1の通信用暗号鍵
(23) 通信用暗号鍵復号化
(24) 通信用暗号鍵受信応答
(25) VPN1内の端末のIPアドレスを入手
(26)
VPN1の通信用暗号鍵による暗号データ通信

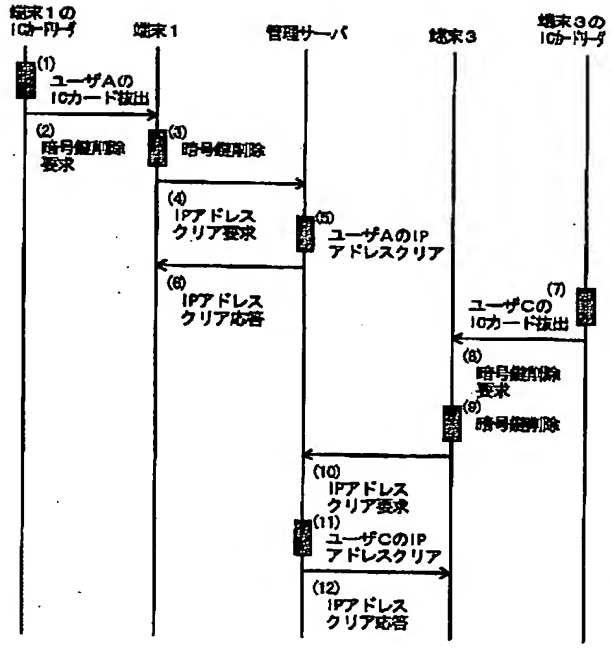
【図４】


端末の処理フローチャート
(A)
START
S1 ICカードから管理サーバの公開鍵とユーザの秘密鍵を読み出す
S2 ユーザIDとパスワードを入力する
S3 ユーザIDとパスワードを管理サーバの公開鍵で暗号化する
S4 暗号化されたユーザIDとパスワードを管理サーバへ送信する
S5 暗号化された通信用暗号鍵を管理サーバから受信する
S6 通信用暗号鍵をユーザの秘密鍵で復号化する
S7 通信用暗号鍵の受信応答を返す
S8 VPN内の端末のIPアドレスを入手する
S9 VPNの通信用暗号鍵による暗号データ通信
(B)
START
S11 ICカードの抜き取り検出
S12 暗号鍵削除
S13 管理サーバへIPアドレスクリア要求
END

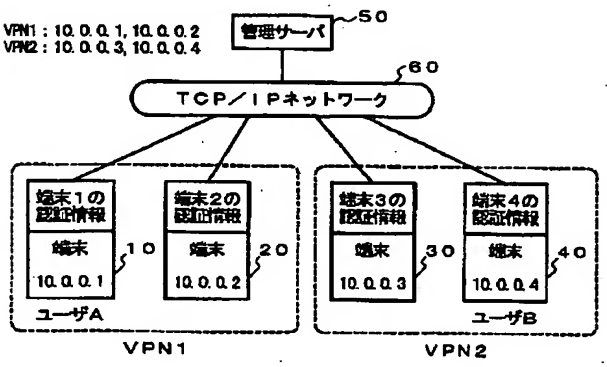
【図５】



【図９】



【図１１】



フロントページの続き

(72)発明者　西條　智幸
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　小野　大泰
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5J104 AA07 AA16 EA19 KA02 MA01
NA02 NA05 NA06 NA33 NA37
PA07
5K033 AA08 CB01 DA01 DB10 DB12
DB14 EC03